

# [UNIX] Multiple Vendor Kerberos kadmind Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00012.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 4 Apr 2007 16:52:45 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Multiple Vendor Kerberos kadmind Buffer Overflow Vulnerability

---

## SUMMARY

<<http://web.mit.edu/Kerberos/>> Kerberos is "a network authentication protocol. It is used in client-server systems to provide user authentication by using a ticket based system. kadmind is the Kerberos administration server. It is used to configure principals and policies on the Kerberos".

Remote exploitation of a buffer overflow vulnerability in the Kerberos kadmind server, as included in various vendors' operating system distributions, could allow attackers to execute arbitrary code on a targeted host.

## DETAILS

Vulnerable Systems:

\* Kerberos version 1.5.1 on Fedora CORE 5

Immune Systems:

\* Kerberos version 1.6.1

## [UNIX] Multiple Vendor Kerberos kadmind Buffer Overflow Vulnerability

The vulnerability exists within the server's logging function, `klog_vsyslog()`. A call is made to `vsprintf()`, with the destination buffer passed as a fixed size stack buffer. User input is not properly validated before being passed to this function, and a stack based buffer overflow can occur.

### Analysis:

Exploitation allows an attacker to execute arbitrary code with root privileges on the targeted host.

In order to exploit this vulnerability, an attacker must have valid credentials stored on the server. Administrator privileges are not necessary. The kadmind server runs on the master Kerberos server. Since the master server holds the KDC principal and policy database, a compromise could lead to a compromise of multiple hosts that use the server for authentication.

### Workaround:

iDefense is currently unaware of any workarounds for this issue.

### Vendor response:

The MIT Kerberos team has made patches available to address this vulnerability. For more information consult their advisory at the following URL:

<<http://web.mit.edu/Kerberos/advisories/MITKRB5-SA-2007-002-syslog.txt>>  
<http://web.mit.edu/Kerberos/advisories/MITKRB5-SA-2007-002-syslog.txt>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0957>>  
CVE-2007-0957

### Disclosure Timeline:

02/08/2007 – Initial vendor notification  
02/08/2007 – Initial vendor response  
04/03/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=500>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=500>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[UNIX] Multiple Vendor Kerberos kadmind Buffer Overflow Vulnerability

[UNIX] Multiple Vendor Kerberos kadmind Buffer Overflow Vulnerability

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.